## III. REMARKS

1. Claims 1-15 remain in the application. Claim 16 has been cancelled without prejudice. Claims 1-4, 6, 7, 9, 14, and 15 have been amended.

2. Claims 2-4, 6, 7, 9, 14, and 15 have been amended to overcome the 35 USC 112, second paragraph rejections.

3. Applicants respectfully submit that claims 1-15 are not anticipated by Dominguez et al. (US 2002/0194138, "Dominguez") under 35 USC 102(e).

3.1 Applicants respectfully submit that Dominguez fails to disclose or suggest:

> a selector configured to be connected to and to receive a control message signal from said second party, said signal including a plurality of selectable communication security protocols for protecting information transmitted over the communication link,
>
> and the selector further configured in response to receiving the control message signal, to select one of the plurality of communication security protocols so that information subsequently transmitted over the communication link between the device and second party is protected using the selected communication security protocol,

as recited by claim 1.

Applicants have differentiated the present claims to encompass a signal that includes protocols for protecting information transmitted over the communication link, as opposed to the distributed authentication options of Dominguez. The "QueryCardholderReq" message received by the cardholder client device is a query regarding whether the cardholder client device has distributed authentication capabilities. The message does not include a plurality of selectable communication security protocols for protecting information transmitted over the communication link.

In response to the "QueryCardholderReq" message, Dominiguez's cardholder client device sends a "QueryCardholderRes" message, which returns "distributed authentication options" to the merchant plug-in. Applicants respectfully submit that returning distributed authentication options is not the same as selecting one of the plurality of communication security protocols.

Paragraph [0034] of Dominguez states that the Payer Authentication Service (PAS) validates participation by the cardholder and cardholder's financial institution and requests a password. Paragraph [0050] states that "Cardholder authentication information includes information such as business identification, country code, card account number, card expiration date, cardholder name, issuer-specific authentication data..., and other information such as billing address, shipping address, social security number, telephone number, account balance, transaction history, and driver license number." There is no selector that selects one of the plurality of communication security protocols in the cardholder client device.

3.2 Applicants respectfully submit that Dominguez fails to disclose or suggest:

> a selector configured for selecting one of a plurality of communication security protocols for protecting information transmitted over the communication link, and being connected to communicate said selection to said second party; and
>
> a calculator for generating a cryptogram for use with the selected communication security protocol, and for transmittal from said device so that information transferred subsequently between the device and second party is protected using the selected communication security protocol.

as recited by claim 14.

Dominguez fails to disclose or suggest a selector configured for selecting one of a plurality of communication security protocols for the same reasons argued above. In paragraphs [0068] and [0069] Dominguez describes sending an offiline PIN that has been authenticated by a chip card EMV cryptogram. Applicants claim is different because it calls generating a cryptogram for use with the selected communication security protocol. In addition, the present claims call for transmittal of the cryptogram from the device, where Dominguez sends the offline PIN.

3.3 Applicants respectfully submit that Dominguez fails to disclose or suggest:

> a receiver configured for receiving a control message signal from the second party specifying a first security protocol for protecting transmitted information;
>
> a calculator configured for generating a second security protocol cryptogram for transmittal from said device to a third party, the third party configured in response to

> receiving the cryptogram, to initiate communication with the second party using the first security protocol so that information transferred subsequently between the third party and the second party is protected using the first security protocol.

as recited by claim 15.

Applicants find nothing in Dominguez that discloses or suggests a receiver for receiving a control message signal from the second party specifying a first security protocol, a calculator that generates a second security protocol cryptogram for transmittal from the device to a third party, where the third party initiates communication with the second party using the first security protocol.

At least for these reasons, Applicants submit that Dominguez does not anticipate independent claims 1, 14, and 15 and dependent claims 2-13.

4. Applicants respectfully submit that claims 1-2, 5, 8-10, 11, and 13 are not anticipated by Williams et al. (US 5,963,924, "Williams") under 35 USC 102(e).

Williams fails to disclose or suggest

> a selector configured to be connected to and to receive a control message signal from said second party, said signal including a plurality of selectable security protocols for protecting information transmitted over the communication link, the selector further configured in response to receiving the control message signal, to select one of the plurality of security protocols so that information subsequently transmitted over the communication link between the device and second party is protected using the selected security protocol,

as recited by claim 1.

Applicants recognize that column 12, lines 49-55 describes a Payment Instruction Applet 200 that delivers order information to a Pay Window Applet 210, 230 on a consumer's desktop. The order information has the same information contained in a Payment Instruction MIME message. Applicants are unsure how payment instructions sent from a merchant to the consumer desktop equates to a signal including a plurality of selectable security protocols for protecting information transmitted over the communication link.

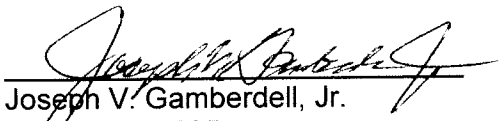
Applicants also recognize that Williams discloses a SET protocol, a CyberCash micro-payment protocol, and a wallet that supports various payment methods, but are unsure how supporting these payment methods equates to a selector configured to receive a control message signal from said second party, said signal including a plurality of selectable security protocols for protecting information transmitted over the communication link.

At least for these reasons, Applicants submit that Williams does not anticipate independent claim 1 and dependent claims 2, 5, 8-10, 11 and 13.

For all of the foregoing reasons, it is respectfully submitted that all of the claims now present in the application are clearly novel and patentable over the prior art of record, and are in proper form for allowance. Accordingly, favorable reconsideration and allowance is respectfully requested. Should any unresolved issues remain, the Examiner is invited to call Applicants' attorney at the telephone number indicated below.

The Commissioner is hereby authorized to charge payment for any fees associated with this communication or credit any over payment to Deposit Account No. 16-1350.

Respectfully submitted,



Joseph V. Gamberdell, Jr.
Reg. No. 44,695

Date

Perman & Green, LLP
425 Post Road
Fairfield, CT 06824
(203) 259-1800
Customer No.: 2512